Chapter 5
Terrorism and Criminal Activities

CHAPTER 5: TERRORISM AND CRIMINAL ACTIVITIES

INTRODUCTION

Unfortunately, every event planner must consider the risks arising from terrorism and criminal activities. The planner must view the event as a potential target and be prepared for any incident. This chapter provides some basic information on terrorism and criminal activities.

Although terrorist and criminal attacks may seem remote possibilities and quite unlikely to occur in the community, event planners and public safety personnel must, nevertheless, plan for their occurrence. Special events and mass gatherings are a perfect target due to the large number of people, media coverage, and the high profile impact if a terrorist hits.

CONTEMPORARY TERRORISM

Prior to the beginning of this decade, terrorism was thought to be something that happened outside the United States and was committed by left-wing extremists to promote ethnic, religious, or socio-economic causes. Before 1993, the United States essentially viewed terrorism as an international event occurring outside this country that sometimes affected U.S. interests. Terrorist acts affecting the United States were primarily directed against United States interests in foreign countries (for example, businesses, military installations, and embassies). The FBI has determined that contemporary terrorists generally:

- Are politically motivated;
- Have sought and used publicity to gain recognition and public sentiment;
- Have most often viewed, trained, and equipped themselves as an army at war;
- Have sought to cross jurisdictional lines to further confound law enforcement detection and apprehension;
- Had the support and funding of national governments from outside the United States; and
- Invited public scrutiny in order to put law enforcement on trial by effective use of the media.

DOMESTIC TERRORISM

The bombing of the World Trade Center in February 1993 led to a new awareness of terrorism in this country - *domestic* terrorism. This event was eventually tied to left-wing extremists of the Palestine Liberation Army who acted in retaliation for American

political, economic, and military support of Israel. With the shift to terrorist events occurring within U.S. borders, a new challenge was created for American law enforcement. The FBI now defines terrorism as:

". . . the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political and social objectives."

Since the World Trade Center bombing, the responsibility for a majority of domestic terrorist activity in the U. S. has shifted from the contemporary international terrorist to the domestic terrorist. For the most part, domestic terrorists can be identified as extremists with strong anti-government feelings. Some are:

- Associated with hate groups;
- Opposed to taxes;
- Defined by religion;
- Ardent believers in a strong constitution; and
- Radical, issues-oriented groups.

Between January 1997 and July 1, 1998, domestic incidents identified as the responsibility of these extremist groups occurred almost daily. The actual number of terrorist acts is probably much larger than the daily count because many law enforcement agencies have not been trained to recognize this activity and probably reported many of these terrorist acts as ordinary crimes.

THREAT ASSESSMENT

Planning and intelligence gathering are necessary activities for law enforcement during event planning. The level of commitment to these anti-terrorist activities influences the level of response capabilities that should be maintained.

Two terms that event planners should understand are anti-terrorism and counter-terrorism:

- Anti-terrorism is a term used to define actions taken to mitigate potential effects of terrorist activity.
- Counter-terrorism is best defined as operational actions taken or activities planned to prevent a terrorist activity or event.

Targets

Most targets singled out by terrorist groups fall into one of five areas:

- Cosmetic or public message targets,

- Non-military government targets,
- Military targets,
- People targets, and
- Cyber-terrorism and information warfare targets.

Each of these targets is usually identifiable within a jurisdiction. Agencies must also keep in mind that the emerging issue of cyber-terrorism allows perpetrators to strike from remote areas anywhere in the world. In 1997 alone, the Pentagon computer system was the target of 6,000 infiltration attempts by computer hackers. The success rate by those hackers was ten percent. This country's air traffic control system and the state's power grid system are vulnerable to terrorist groups who are sufficiently knowledgeable to infiltrate these systems.

Motives

The motives of extremist groups can generally be identified as:

- Political,
- Religious,
- Racial,
- Environmental, or
- Special interest.

Weaknesses in Measuring Threat

Terrorist threats are often difficult to measure because they are:

- Dynamic,
- Mobile,
- Difficult to recognize (lone offenders, splinter groups),
- Ease and availability of creating a WMD device, and
- Difficult to quantify-subjective (open to interpretation, tendency towards inflating results).

Dangers of information sharing (outside the law enforcement community) also make it difficult to measure the extent of the threat because unauthorized disclosure of information may:

- Lead to violation of operational security;
- Create unnecessary panic; and
- Produce unintended media attention.

Basis of the Assessment Process

Capability and Intent = Threat
Threat and Vulnerability = Risk
Risk and Capabilities = Needs

The United States Congress based their decision largely on advice from the U.S. General Accounting Office, who opined that the particular assessment process look at the capabilities and intentions of specific subject groups and / or individuals when assessing the threat. This represents the foundation of the threat process well known to the law enforcement and intelligence communities.

Based on this foundation, the assessment process was developed. This process looks at the capability to produce and deploy a WMD and the intent of a specific threat element to do so. Without the mutual existence of capability and intent, no imminent threat can be said to exist. Once relative threat levels have been established, an assessment team may assess the risk to a particular jurisdiction. This involves the evaluation of existing vulnerabilities to safeguard and prevent an attack in a particular jurisdiction against the existing threat.

VULNERABILITY ASSESSMENT

In the cases of the jurisdictional domestic preparedness strategy development process, it is the selection of your critical infrastructure and applying seven factors to that infrastructure to determine weaknesses in your jurisdictional capability to respond to the incidents covered by your Jurisdiction Emergency Response / Operations Plan. These vulnerabilities are specifically directed at WMD terrorism or WMD incident response.

This assessment is a critical part in the development of the jurisdiction strategy and determines an internal environmental factor for the jurisdiction to improve their capability to respond to a WMD terrorism or WMD incident. This focuses the jurisdiction's ability to take care of its citizens.

The outcomes of this assessment will be an inventory of the critical infrastructure within the jurisdiction and a assessment of how easily it can be disrupted.

STATE ROLES IN READINESS AND RESPONSE

An integrated approach between the local, state, and federal government makes a logical clearinghouse for intelligence on the movement and activities of terrorist groups and the collection, interpretation, and dissemination of that information to the proper enforcement agencies. A proactive role in planning and intelligence gathering will lessen the likelihood of a surprise emergency incident, which improperly handled can make or

break a department and its administrators at all levels of government. Descriptive intelligence with predictive interpretation that forecasts the probability of threat and target can enhance operational readiness in training, equipping, and practicing to respond to emergency incidents. If nothing else is done by law enforcement in the intelligence area, threat assessment must be considered, at a minimum. Planners must have appropriate contacts and phone numbers at hand before the event.

State law enforcement agencies should take the lead in pre-incident threat forecasting and planning. Roles and responsibilities of the various stake-holding agencies for the event being planned need to be determined and an incident chain of command put in place, so that, should a terrorist threat materialize, confusion and duplication of response can be diminished.

HIGH PROFILE/CONTROVERSIAL EVENTS

Due to the nature of the event, the crowd composition, or for other reasons, certain events cause more controversy and create greater risks than others do. For example, events involving groups which holds controversial beliefs, present a greater risk for criminal or terrorist behavior. Events involving high level officials are also at a greater risk for terrorist activity because of the significance of the official and the high-profile visibility of the participants and those in attendance. On some occasions, if the date of the event coincides with the anniversary of another terrorist event, the date of the event itself may be considered controversial. Planners must consider every reason why an event may promote controversy or attract special attention.

Conflicts will exist between public safety, recovery, and criminal investigation agencies during terrorist incidents. Rescue and recovery issues and actions must be separated from criminal investigation issues and actions before the event occurs, and non-law enforcement workers should be given training on matters of evidence. Evidence teams should be created to practice and train with local emergency responders to promote mutual understanding of one another’s roles.

FEDERAL ROLES AND RESPONSIBILITIES

One of the best ways to combat terrorism and criminal activities is to identify ahead of time the potential threats and prepare for them. The FBI is the lead agency in addressing terrorism and providing information about terrorist groups in the United States. The FBI may request assistance from federal agencies if needed. The Nunn-Luger-Domenici legislation passed in 1996 funded efforts to assist communities in the preparation against WMD terrorism.

Under Presidential Decision Directive (PDD) 39, the FBI is the lead-agency for crisis management and response to terrorist incidents while FEMA is the lead agency for consequence management. **However, the first response to any of these events will always be the local response**. The FBI can summon extensive federal resources for use at an event, but local responders will be on their own until the FBI arrives.

The FBI has created internal specialized terrorism units with responsibility for:

- Domestic terrorism,
- Weapons of Mass Destruction (WMD),
- Special events,
- WMD countermeasures,
- Computer investigations/operations, and
- Field multi-agency Joint Terrorism Task Forces to work with state and local enforcement.

Develop a relationship with the FBI WMD coordinator to learn about terrorist groups and whether your date or event holds a special significance that may put your event at excess risk.

B-NICE

The B-NICE threat of weapons of mass destruction is currently a much-discussed topic in this country. The Federal government is prepared to assist communities in the event of a terrorist attack. The U.S. Government states that it will use all means to deter, defeat, and respond to terrorist attacks. It will make no concessions to terrorists; it will identify terrorists and punish them, and it will work closely with other agencies to carry out U.S. policies and to combat threats.

Since 1990 the U.S. Government has passed the Biological Weapons Anti-terrorism Act (President Bush, 1990), and the Use or Attempted Use of Weapons of Mass Destruction Federal Statute to combat WMD and to provide appropriate penalties for individuals caught possessing or using these weapons. These statutes were tested in this country for the first time following the Oklahoma City bombing.

The Department of Defense has created Weapons of Mass Destruction Civil Support Teams to assist the FBI and communities facing terrorist attack. These teams are made up of National Guard members who assist in the detection and identification of WMD. Since these teams are composed of National Guardsman, governors may also deploy teams to assist communities. The local community's first responders will still assist, but if the attack is beyond their capability, they may seek assistance from the state or federal government.

Intelligence gathering, threat assessment, containment of potential threats, and effective planning for crisis and consequence management prior to a mass gathering or special

event are of central importance to a jurisdiction having the ability to effectively prevent or counter these threats.

A Weapon of Mass Destruction (WMD) is:

- Any weapon that is designed or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals, or their precursors;
- Any weapons involving a disease organism; or
- Any weapon that is designed to release radiation or radioactivity at a level dangerous to human life.

Other terms associated with WMDs are:

Secondary Device

A secondary device is usually explosive and designed to injure first responders when they arrive at an incident. Following the arrival of the first responders, a second device explodes in the responder area. A secondary device was recently used at an abortion clinic explosion.

Anti-personnel Devices

Anti-personnel devices are used to injure people and may or may not be considered secondary devices that target responders.

Specific Threat

A specific threat explains what will occur, for example, "A bomb will go off in one hour in the parking garage."

Non-specific Threat

A non-specific threat does not explain what may occur, for example, "Everyone in the building is going to die."

Capability

Capability refers to credible information that a specific group possesses the requisite training, skills, financial means, and access to resources necessary to develop, produce, or acquire a particular type of WMD in a quantity or potency sufficient to produce mass casualties, combined with information substantiating the group's ability to safely store, test, and deliver the same.

Projected National Threat

Interest in WMD material will continue to increase. Explosives, shootings, and kidnappings will remain the most likely terrorist options. The threat of hoaxes, blackmail, and mass disruption is high.

BIOLOGICAL

Biological terrorism is not a new type of warfare. Biological agents are by far the most dangerous of the three types of weapons of mass destruction. Agents include bacteria, fungi, viruses, or toxins that induce disease or death in any living thing.

The difficulty in countering biological terrorism begins with identifying it. Another serious concern arising from the use of all biological agents is the time that can elapse before their use by terrorists is discovered. Biological attacks can be slow acting, with the symptoms not showing up until as many as 10 days after exposure. The further contamination of additional population by those initially exposed multiplies exponentially as time from the initial exposure increases. The best defense against the spread of the biological element is accurate documentation and tracking of this kind of WMD by medical personnel to contain the exposure.

One case highlights the importance of intelligence sharing between federal, state, and local authorities. The Minnesota Patriots Council in 1990 is known to have created the biological agent Ricin and plotted to use it against a Federal marshal. The plot was thwarted when a county sheriff arrested the wife of one member of the group on unrelated charges, and she revealed the plot and the location of the biological agent. At the time the biological agent was taken as evidence, the group had enough powdered Ricin to kill 125 people relatively easily.

With many countries facing economic difficulties at the end of the Cold War, experts fear that they may be selling their biological weapons to the highest bidder. However, the lack of an effective delivery system to deploy a biological agent currently limits the ability for widespread impact upon the population.

NUCLEAR

Nuclear terrorism refers to the use of nuclear or radiological materials as weapons or to cause damage. This threat creates the largest challenge for law enforcement into the new millennium.

Although the use of a crude nuclear weapon makes the threat of nuclear terrorism possible, FBI intelligence suggests that it would be difficult for a group to construct such a weapon without weapons-grade uranium or plutonium, which are currently strictly regulated in this country. Nuclear terrorism, then, does not pose a credible immediate threat.

Since nuclear weapons are more easily detected, responders know what they are dealing with. As with the other WMD, the best defense is to have a plan and practice it.

INCENDIARY

Incendiary devices have been used by terrorists for many years since it is a flexible tool capable of causing property damage, loss of life, and panic. Incendiary devices continue to spread until fuel is gone or it is extinguished.

Information from the FBI Bomb Data center reports that incendiary devices were used in approximately 20-25 percent of all bombing incidents in the United States and that when used, incendiary devices ignited approximately 75 percent of the time.

They also reported that less than 5 percent of actual or attempted bombings were proceeded by a threat. The lack of prior notification makes casualties more likely than if a notice is given.

Incendiary devices can be classified as:

- Chemical reaction (including burning fuse)
- Electronic ignition
- Mechanical ignition

The type and construction is only limited to the creativity of the builder.

Incendiary devices may be stationary (placed), hand-thrown (Molotov cocktail), or self-propelled such as rockets or rifle grenades.

The components of an incendiary device are the ignition source, combustible filler material, and housing or container.

The device may be made of:

- Roadway flares,
- Gasoline and motor oil,
- Light bulbs,
- Common electrical components and devices,
- Matches and other household chemicals,
- Fireworks,
- Propane and butane cylinders, and
- Plastic pipes, bottles, and cans.

DETECTION

To detect an incendiary device combustible gas meters, flame ionization detectors, trained dogs, photoionization detectors, and calorimetric tubes may be used.

The clues are similar to detection clues for arson. The clues should be a signal for the responder to take appropriate actions to safeguard himself and the public and treat the area as a potential crime scene. The signs include:

- Prior warning (phone calls),
- Multiple fire locations,
- Signs of accelerants,
- Containers from flammable liquids,
- Splatter patterns indicating a thrown device,
- Fusing residue,
- Signs of forced entry to the area, and
- Common appliances out of place for the environment.

EXPLOSIVES

Explosives seem to be the weapon of choice for terrorists. The explosives can deliver an assortment of destruction and provide a vehicle for dispersal of chemical, biological, incendiary, and nuclear agents.

Explosives produce four effects when detonated:

- Blast pressure-There are two different phases of blast pressure. Positive blast pressure (overpressure) move rapidly away form the explosion center (ground zero) due to the expansion caused by the release of energy. After the positive pressure phases, a vacuum is created at the explosion site. This creates a negative pressure that moves toward the original center of the detonation at hurricane speed. It is less sudden, but last approximately three times as long as the positive pressure wave.

- Fragmentation-An explosive device may propel fragments at high speed for long distances. This often accounts for many injuries or casualties.

- Thermal effect- Sometimes referred to as the incendiary effect, heat produced by the detonation of either high or low explosives varies according to the ingredient materials. High explosives generate greater temperatures than low explosives. However, the thermal effects from low explosives have a longer duration then those of high explosives. The thermal effect is visible in the bright flash or fireball temporarily produced by an explosion. Thermal effects vary as to type of explosive, container, addition of fuel/accelerants, shielding, and proximity.

- Ground Shock-Ground, or seismic shock, is possible but usually will only be generated by a large detonation.

Explosives are defined as materials capable of violent decomposition. This decomposition often takes the form of extremely rapid oxidation (burning). Explosions are the result of sudden and violent release of gas during the decomposition of explosive substances. High temperature, strong shock, and a loud noise follow this release. Explosives are classified according to the speed of their decomposition.

CHEMICAL

Chemicals may be used as weapons or to deliver an attack. Originally, the military designed chemical weapons to use in wartime. The results of chemicals used as weapons were so devastating in warfare that many countries rejected their future use and created treaties to forbid their future use and manufacture. In 1995 terrorists attacked a Tokyo subway. Twelve persons died, 4500 were injured, and over 700 required extended hospital stays. The ease of access to chemical agents and the amount of damage they cause make chemical warfare very appealing to radical groups. Directions for the creation and use of chemical weapons can be found on the World Wide Web.

Chemical agents include nerve agents, blood agents, choking agents, and blister agents. These chemical weapons have been used in the recent past both within the United States and abroad. These agents do create a credible threat for use by extremist groups in this country, and there is a high probability that chemical agents are likely to be encountered by state and local law enforcement of this country in the future.

Responders must be prepared to manage a terrorist attack involving a chemical agent. To prepare, they should become knowledgeable of the range of chemical agents used by terrorists in the recent past. Knowledge of chemicals and their effects assists in the first stages of treatment. Each community should establish chemical weapons attack response plans and review them regularly.

EXPLOSIVES

Since they are readily available, explosives are the most common weapons of mass destruction. When you plan an event, find out who the responder is for possible explosives or suspicious packages. Does your community have a bomb squad? Do you have dogs that are trained to identify explosives? What is the community policy on explosive devices? Plan ahead and know who to call in an emergency.

MITIGATING ACTIONS

Unattended Packages

At every event, people will leave some items unattended. Public safety officials must decide beforehand how to handle these items. Who will respond? Does the community have dogs trained to identify explosives? Will the area be evacuated? Decide these issues ahead of time and have a written plan for all public safety personnel to follow.

Concealment Areas

Concealment areas are areas where persons may hide, or where someone may hide packages or other weapons. The best way to avoid problems in these areas is to map the event grounds and identify the areas that could be used as hiding spots. The venue staff could assist police in this matter.

Security Sweeps

How often is security going to go through the event site? What are they looking for? How do they handle incidents? Who is going to do the sweep? Venue personnel and security personnel should work together. These are a few areas to address in advance. Once a sweep of the area has been done the area must be secured.